CLAIMS

WHAT IS CLAIMED IS:

1. A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;

an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and

a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:

directing incoming electronic mail from the internet backbone to the scanning system.

2. A network security system according to claim 1, further comprising:

a decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications received via the internet backbone;

wherein the switch is further coupled to the decoy server and is further configured for redirecting suspicious traffic from the internet backbone to the decoy server.

3. A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;

a mail proxy server for determining whether the incoming electronic mail is to be scanned for malicious code and directing the incoming electronic mail to the scanning system when thee incoming electronic mail is determined to be scanned for malicious code;

an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and

a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:

directing incoming electronic mail from the internet backbone to the mail proxy server.

4. A network security system according to claim 2, further comprising:

a decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications received via the internet backbone;

wherein the switch is further coupled to the decoy server and is further configured for redirecting suspicious traffic from the internet backbone to the decoy server.

5. A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a plurality of scanning systems coupled to the intranets for scanning incoming electronic mail for malicious code;

a plurality of anti-virus servers coupled to the intranets for downloading anti-virus code to clients coupled to the intranets;

a plurality of switches coupled between the internet backbone, the scanning systems, and the anti-virus servers, said switches configured for:

directing incoming electronic mail to at least one of the scanning systems.

6. A network security system according to claim 5, wherein the switches are further configured for:

load-balancing among the scanning systems and among the decoy servers.

7. A network security system according to claim 5, further comprising:

a plurality of decoy servers coupled to the intranets for masquerading as legitimate servers and logging activity on communications received via the internet backbone;

wherein the switches are further coupled to the decoy servers and are further configured for redirecting suspicious traffic from the internet backbone to the decoy servers.

8. A method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

directing incoming electronic mail from the internet backbone to a scanning system;

scanning incoming electronic mail for malicious code; and

downloading anti-virus code to clients coupled to the intranets.

9. A method according to claim 8, further comprising:

redirecting suspicious traffic from the internet backbone to the decoy server;

simulating the decoy server as a legitimate server to the suspicious traffic; and

logging activity on communications received via the internet backbone.

10. A method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

directing incoming electronic mail from the internet backbone to one of a plurality of mail proxy servers;

at the one of the mail proxy servers, determining whether the incoming electronic mail is to be scanned for malicious code and directing the incoming electronic mail to a scanning system when the incoming electronic mail is determined to be scanned for malicious code;

at the scanning system, scanning incoming electronic mail for malicious code;

downloading anti-virus code to clients coupled to the intranets.

11. A method according to claim 10, further comprising:

load-balancing among the mail proxy servers.